UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,291	08/16/2001	Marinus Frans Kaashoek	12221-005001	3137

26161 7590 05/02/2006

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 05/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,291	KAASHOEK ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) *2,10,20 and 23* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-9,11-19,21,22 and 24-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 August 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's argument regarding applied reference, Malan USPN 6,944,673, on the Office Action mailed on 09/26/2005 is moot. Examiner applies new grounds of rejection.

2. The Applicant states that Messmer says nothing about a control center that coordinates thwarting of attacks. The Examiner disagrees. Counterpane data center is used for a managed security service to identify DOS attacks or other threats. The Counterpane data center receives network activities from monitors/Counterpane box to determine if a consumer system/victim data center is under DOS attack (see, lines 1-20).

3. The Applicant states that Messmer's article teaches away from this feature by stating that: "Counterpane staffers advise corporations on how to combat threats but do not make changes to the corporation's equipment." The Examiner disagrees. Messmer teaches a managed security service of counterpane data center that identifies DOS attack based on information captured by monitors and transmitted to counterpane data center through different network (see, lines 5-49).

4. The Applicant states that Messmer fails to suggest "sending data collected from the network over **redundant** network, with the redundant network being a physically separate network from the network that the plurality of monitors collect data from." The Examiner disagrees. The monitors/counterpane box collects data from the network over a hardened redundant network and/or different networks (see, lines 23-28).

5. The Applicant states that Messmer fails to suggest the feature of a process... to analyze the data from the plurality of monitors to determine network traffic statistics that can identify

malicious network traffic. The Examiner disagrees. Messmer discloses receiving attack information from monitors/counterpane box and analyzing the received information to determine and identify the DOS attack on the target consumer/victim data center (see, lines 4-32).

6. The Applicant states the Examiner's acknowledgement for Messmer being silent on analyzing and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center. Argument is moot in new grounds of rejection.

Drawings

7. The drawings are objected to under 37 CFR 1.83(a) because they fail to show "software program 21" on page 5 lines 7-8 of Fig. 1, as described in the specification. Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner,

the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Double Patenting

8. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

9. Claims 1, 3-9, 11-19, 21-22, 24-27 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-36 of copending Application No. 09/931,561. Although the conflicting claims are not identical, they are not patentably distinct from each other because the application '561 teaches all the claims limitation except the differences that are underlined in the following table as an example:

Instant application 09/931291	**Copending application 09/931,561**

1. A system, comprising: • a **control center** to coordinate thwarting attacks on a victim data center that is coupled to a network, the control center including: • a communication device to receive data from a **plurality of monitors**, dispersed through the network, with the monitors sending data collected from the network, with the monitors sending data collected from the network over a redundant network, with the redundant network being a physically separate network from the network that the plurality of monitors collect data from; • a computer system, the computer system comprising: • a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic; and • analyzes and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center.	1. A method of thwarting denial of service attacks on a victim data center coupled to a network, the method comprising: • monitoring network traffic through **monitors** disposed at a plurality of points in the network; • communicating data from the monitors to a **central controller**, over a redundant network, that is a different network from the network being monitored; • analyzing the data comprising network traffic statistics to identify network traffic that is pert of a denial of service attack; and • filtering the network traffic based on results of analyzing the network traffic to discard network traffic that is identified as part of the denial of service attack. 5. The method of claim 3 wherein monitoring network traffic through the gateway occurs at network entry points of victim data centers.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

10. The only difference between these two applications is that the copending application '561 has a broader claim limitation as underlined above and the instant application has narrower claim limitations. Wherein said identifying malicious traffic applicant describes the identifying

malicious traffic and/or denial-of-service (DOS) being identical in the process (see, page 17 last paragraph) and the action performed upon identifying the DOS/malicious traffic being discarding network traffic and eliminating the malicious traffic are interpreted explicitly the same. And further applicant's protection of victim's data center is claimed on dependent claim 5 as shown above.

11. Claims 1, 3-9, 11-19, 21-22, 24-27 of the instant application are envisioned by copending Application No. '561 claims 1-36 in that claims 1-36 of the copending application contain all the limitations of claims 1, 3-9, 11-19, 21-22, 24-27 of the instant application. Claims 1, 3-9, 11-19, 21-22, 24-27 of the instant application therefore are not patently distinct from the copending application claims and as such are unpatentable for obvious-type double patenting.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

13. Claims 1, 9, 18, and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Greenwald et al. US PG PUBs 2003/0149919 A1.

Regarding claims 1, 9, 18, and 21 Greenwald et al. teaches a system, comprising:

a control center (**fault diagnosis engine**) to coordinate thwarting attacks (par. 0032; ***fault including Denial of Service Attacks***) on a victim data center that is coupled to a network (par. 0034 and fig. 2A; ***target***), the control center including:

a communication device (par. 0072; ***receiver fault diagnosis engine***) to receive data from a plurality of monitors (***plurality of fault engines*** *on fig. 3 element 150*), dispersed through the network, with the monitors sending data collected from the network , with the monitors sending data collected from the network over a redundant network, with the redundant network being a physically separate network from the network that the plurality of monitors collect data from (par. 0032, 0025 and fig. 6; ***in a physically different network***);

a computer system, the computer system comprising:

a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic (par. 0032 and 0035; ***determination of faults/DOS by fault engines and fault diagnosis engine***); and

analyzes and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center (par. 0032, 0104 and fig. 6B-C; ***packet filtering, monitor gateway preventing traffic from being***

transmitted from first to second device upon detection). And dependent claims are rejected based on dependency and/or other rejection in this Office Action.

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 1, 3, 5-6, 9, 12-13, 18-19, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Messmer in view of Yavatkar et al. USPN 6,735,702 B1.

As per claims 1, 9, 18, 21, Messmer teaches a central control center (i.e. Counterpane data center)(see lines 26-28) to coordinate thwarting attacks(see lines 1-20), coordinating thwarting attacks is taught in Messmer, because Messmer teaches that the data center monitors network traffic to determine if the customers network is under attack. Messmer teaches a victim data center, because Messmer teaches that outsourcing intrusion detection, one company that does this is Counterpane, Counterpane monitors customers network (see lines 12-15), the customers network is the victim data center. Messmer teaches a communication device (i.e. probe/black box)(see lines 17-26) to receive data from a plurality of monitors (see lines 23-26), dispersed through the network (see lines 23-27), the monitors sending data collected from the network over a hardened redundant network (see lines 23-28), Messmer teaches a hardened redundant network because the data collected is sent in encrypted form to the central control center (see lines 23-28).

Messmer teaches the redundant network being a physically separate network from the network that the plurality of monitors collect data from, because the plurality of monitors are on the customers network (12-26), the central control center has its own network, that is in California or Virginia, where the data from the monitors is collected and sent to the data center (see lines 26-28). Messmer teaches a computer system that includes a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic (see lines 28-32).

Messmer is silent on, filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center. However, Yavatkar et al. discloses analyzing traffic on a network by monitoring network traffic when a particular network attack is detected by gathering information about the traffic on the network through redundant network (see, fig. 2), by launching an agent and having the agent iteratively identify which of the links on the node on which agent operates accepts a type of traffic, and traversing the identified link to the node across the link by halting, closing the path, shutting down, and/or installing appropriate filter on the monitor gateway (see col. 13 lines 54-col. 14 lines 32). It would have been obvious to one of ordinary skill in the art at the time of the invention to include Yavatkar et al.'s filtering process and eliminate the malicious traffic from entering the victim data center within the system of Messmer because it would block the attack targeted on the victim's computer. One would have been motivated to do so because it would further secure the victim's system from malicious attack that is sent over the hardened network.

As per claim 3, Messmer further teaches wherein the data analyzed by the control center is

collected statistical information about network flows (see lines 29-30).

As per claim 5, Messmer further teaches wherein the control center is a hardened site, because the data collected is sent in encrypted form to the central control center (see lines 23-28). Messmer teaches the redundant network being a physically separate network from the network that the plurality of monitors collect data from, because the plurality of monitors are on the customers network (12-26), the central control center has its own network, that is in California or Virginia, where the data from the monitors is collected and sent to the data center (see lines 26-28).

As per claim 6, Messmer further teaches wherein the monitors include gateways that are disposed at the victim data center and data collectors that are disposed in the network (see lines 12-25), the analysis process executed on the control center analyzes data from gateways and data collectors dispersed throughout the network (see lines 26-30).

As per claims 12, 19, Messmer further teaches receiving and analyzing are performed by a control center coupled to the data collectors via the hardened, redundant network (see lines 12-28).

As per claim 13, Messmer further teaches wherein plurality of monitoring devices (see lines 13-26); are data collectors dispersed throughout the network and at least one gateway device that is disposed adjacent the victim site to protect the victim (see lines 6-26), and wherein analyzing includes analyzing at a control center data from the at least one gateway and the data collectors dispersed throughout the network (see lines 26-30).

Same Motivation applies above (see claim 1). Claim 18, is rejected under the same basis as claim 1. Further, Claim 18, is rejected for Malan disclosing determining a filtering process to eliminate the malicious traffic from entering the victim center; and aggregate traffic information and coordinating measures to locate and block sources of an attack (see col. 4, lines 60-65, col. 5, lines 43-53, col. 7, lines 1-6).

As per claim 21, limitations have already been addressed (see claims 1 and 18).

16. Claims 7-8, 14-16, 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Messmer in view of Yavatkar et al. USPN 6,735,702 B1 and further in view of Hill et al.

As per claims 7, 14, 24 Messmer does not disclose classifying attack. However, Hill et al. does disclose classifying attacks (see col. 5, lines 66-67, col. 6, lines 1-18). It would have been obvious to one of ordinary skill in the art at the time of the invention to include Hill et al. classifying attacks within the combination system of Messmer and Yavatkar et al., because classifying attacks displays attack information in a usable and quickly interpretable form to a network manager while minimizing the loading on the computer (see col. 2, lines 45-50 of Hill et al.). Therefore, by classifying attacks provides a network manager with knowledge of the severity and overall nature of the attack (see col. 2, lines 53-60 of Hill et al.).

As per claims 8, 15, 25 same motivations as above. Hill et al. further discloses wherein the classes of attack are denoted as low-grade with spoofing, low-grade without spoofing and high-

grade whether spoofing or non-spoofing (see fig. 3, sheet 3, fig. 7, sheet 6).

As per claim 16, Messmer further teaches sending requests to gateways to send data pertaining to an attack to the control center (see lines 14-27).

Conclusion

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.
April 28, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

4/30/06